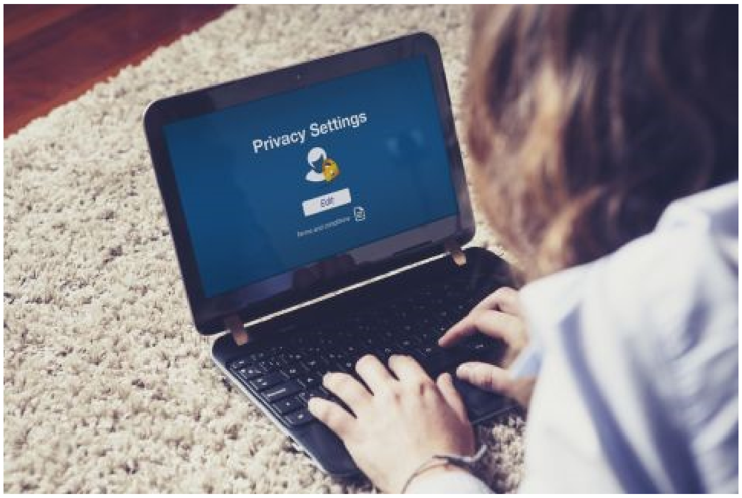
Looking ahead – data privacy best practices in 2019

www.itproportal.com
4 mins read



In 2018, data privacy was at the forefront of consideration for leadership teams spanning across all industries. From large scale data breaches, to the introduction of new data privacy regulations like the General Data Privacy Regulations in Europe, the limits of existing data management strategies were tested. As we kick off this new year, we shouldn't expect the focus on data privacy efforts to shift very much. There have already been conversations about the potential for a federal data privacy law here in the United States and we have already begun to see States, most recently California, begin to pass their own legislation. In preparation for the coming year, there are a few strategies organisations should be considering, to ensure successful data management best practices.

The root of compliance challenges

In recent survey of IT professionals, results found that only 22 per cent of those questioned felt their organisations sufficiently address information management and privacy needs – which is an issue for a few different reasons. When it comes to data privacy, from a historical sense, the United States has typically been a few steps behind Europe. The European Union has long had a progressive stance on privacy, which is something we have not been seen in this country yet. However, the California Consumer Protection Act might be the fire needed to fuel the flame in 2019.

Additionally, at the 40th International Conference of Data Protection and Privacy Commissioners in Brussels last year, C-Suite executives of potentially the three largest technology companies in the world, Apple, Facebook and Google, all made strong commitments to data privacy in the forthcoming year. There was a clear admission that what had happened in 2018 was no longer acceptable. One of the key takeaways was that Tim Cook, Erin Egan and Sundar Pichai, all gave their full support to a federal data privacy law in the United States. This public declaration of support was a step in the right direction from the perspective of most in the audience.

One of the other issues around compliance is that many companies, especially ones that do not conduct business globally, have not been previously required to comply with legislation as strict as GDPR. As we have watched the role of data evolve over the past few years, companies have struggled to keep up with the expectations that came with these changes. Whether that meant dealing with electronic records instead of physical file cabinets or being able to provide a tamper-proof audit trail for litigation, demands were constantly changing, which has led organisations to purchase various technologies to handle each individual demand.

However, full-fledged information management and privacy has completely different requirements. The most practical solution in this case is to provide consistent management across the enterprise, which is a relatively new approach. Organisations should consider a consistent solution to manage data in a way that has previously been resisted for almost two decades. Of course, this solution will not be a quick and easy fix for a larger scale issue, given it requires the involvement of multiple business groups, which is no small task.

Dealing with compliance best practices

Once companies can determine their information management needs, the next step is to conduct a review of their existing information governance strategies. As previously mentioned, data privacy programs require consistent attention across all business functions – from the marketing department, ranging through to the legal and finance teams. One of the most useful functionalities of data is that it is not hindered by geographical or physical boundaries. That being said, data management solutions must be able to transcend across all facets of the company, which has proven to be a daunting task. It is important for companies of all sizes to break down these projects into smaller milestones, in order to set up a successful information governance program. A few steps that should be considered, include:

Communication and collaboration are key: One of the best ways to take control of your organisation's data is to establish an internal task force that focuses on information governance and data privacy specifically. Each team within the company, from records, legal, IT, risk, compliance even up to the C-suite level, should have representation in order to ensure organisation-wide alignment.

Take charge of the data Does your organisation know how many applications are managing data and where all that data resides? Determining a road map of potential vulnerabilities to focus on first, before moving your focus to less-vulnerable areas is a great place to start. Once all data sources have been analysed, the organisation is informed and ready to make a educated decision.

Enact policy changes Once an organisation has identified its data sets, the next step is to officially change the policy and implement a solution that will ensure this policy is actually enforced and done so in an efficient manner. Many organisations have changed their policies to comply with privacy regulation, which is a very positive initial step, but if an organisation cannot enforce the policy, then there was really no point in implementing it from the start. This policy change is usually considered a records management task, but organisations must start managing existing data, while understanding that volumes of new data will be generated constantly, further proving the point of why companies need a plan of action to avoid constant reorganisation.

So, what's next for data privacy?

Whether we receive a piece of federal legislation or not, just keeping up with the multitude of new regulations and understanding what they mean in the context of each organisation will be most likely be a difficult task.

Given the fact that many organisations are conducting business globally, laws like the GDPR, DPA 2018, Argentina Data Protection Laws, Brazilian Data Protection Laws, Convention 108 and Brexit all must be considered, when monitoring the flow of international data. It's tough to comprehend what these laws mean, but more importantly what changes must take place in order to be compliant. Buy-in from the entire organisation is necessary and if an organisation doesn’t have an information governance program in place, it’s a very important and logical place to get started.

Callum Corr, Data Analytics Specialist, ZL Technologies
Image Credit: David M G / Shutterstock

■